GIBSON DUNN

Gibson, Dunn & Crutcher LLP

200 Park Avenue
New York, NY 10166-0193
Tel 212.351.4000
www.gibsondunn.com

Kate Dominguez
Direct: +1 212.351.2338
Fax: +1 212.716.0839
KDominguez@gibsondunn.com

April 19, 2022

Hon. Jeremiah J. McCarthy
United States Magistrate Judge
Robert H. Jackson United States Courthouse
2 Niagara Square
Buffalo, NY 14202

Re: *Moog Inc. v. Skyryse, Inc. et al.*, Case No. 1:22-cv-00187

Dear Judge McCarthy,

As directed by the Court at the April 8, 2022 telephonic hearing, the parties met and conferred on the issues Moog raised in its April 7, 2022 letter to the Court. Following those meet and confers, two issues remain unresolved. Accordingly, and pursuant to the Court's April 8 and 18, 2022 Orders (Dkts. 58, 72), we respectfully submit this letter on behalf of Defendant Skyryse, Inc. to address the parties' disputes regarding (1) a forensic protocol, and (2) the Attorneys-Eyes-Only provisions of a stipulated protective order. We are available to discuss this further at the Court's convenience.

Forensic Inspection Protocol

As Skyryse has told Moog since the beginning of this action, Skyryse does not want any of Moog's trade secret information and has never had any intention of acquiring it. To the extent any Moog information reached Skyryse, Skyryse wants to return that information. That is why, within days of learning of Moog's allegations, Skyryse agreed to search for and return any non-public Moog information in Skyryse's possession, and promptly took diligent steps to investigate Moog's claims, search for Moog's data, and return any non-public Moog data that could be identified. That agreement is reflected in the March 11, 2022 Stipulation and Order (the "March 11 Order") agreed by the parties and entered by the Court.

As reflected in the March 11 Order, although the parties agreed that Skyryse would deliver to Moog any of Moog's non-public information in its possession, the parties recognized the possibility that Moog's information could have been integrated or stored with *Skyryse's* non-public and trade secret information in such a way that Moog's information could not be delivered to Moog without delivering Skyryse's information at the same time. *See* March 11 Order (Dkt. 25) at 2. Accordingly, the parties agreed that if any of Moog's non-public information were used in such a way that delivery of Moog's information would "necessarily include[] property of any Defendant," that information would not be delivered to Moog. *Id.* Instead, Skyryse would deliver that information to a mutually agreed-upon third-party neutral forensics firm, "*in lieu of* providing such information *directly to Plaintiff*." *Id.* (emphases added).

At Moog's recommendation, the parties selected third-party iDiscovery Solutions ("iDS") as the third-party neutral. And in accordance with the March 11 Order, Skyryse produced to iDS Defendant Kim's Skyryse-issued laptop, and 11,093 files found on Defendant Pilkington's Skyryse-issued laptop. The individual defendants delivered to iDS 23 additional devices.

The March 11 Order also sets forth the process by which the information delivered to the third-party forensics firm would be handled. Under the Order, the parties shall "agree on a protocol for searching all such information delivered to the Forensics Firm for use in discovery in the above-titled matter." *Id.* at 3. Following that mandate, the parties exchanged proposed forensic protocols for the devices provided to iDS. Exs. 1–2.

The parties' proposals reflect two fundamentally different views over who should be entitled to search the information delivered to iDS and how. Consistent with the express purpose of engaging the neutral forensics firm—*i.e.*, so that Skyryse's sensitive information would *not* be delivered directly to Moog—Skyryse wants *iDS* to search for Moog's non-public and trade secret information on the devices and provide the results of those searches to the parties. In contrast, and contrary to the March 11 Order, Moog wants its expert and outside counsel to have unfettered, *direct* access to the *entirety* of the forensic images of the devices with iDS, unrestricted by any search terms at all—let alone search terms designed to identify any purported Moog non-public information or trade secrets.

Skyryse's proposed protocol—to which the individual defendants agreed—is consistent with those endorsed by courts across the country in trade secrets cases, and properly balances Moog's interest in obtaining relevant discovery with Skyryse's interest in protecting privileged and proprietary information on its devices. Requiring iDS to conduct searches of the devices for Moog's purportedly non-public information, as identified by Moog, is customary. And Skyryse nonetheless offered during the parties' meet and confer to add a provision to permit iDS to conduct *additional* searches using search terms agreed between the parties.

Moog's unbounded protocol, by contrast, gives Moog unfettered access to Skyryse's information and devices in a manner no different from if the information had been delivered directly to Moog—precisely what the neutral forensics firm was designed to avoid. Moog's proposal is unprecedented; courts do not grant a trade secret plaintiff complete access to a defendant's systems. And it flies in the face of the March 11 Order which, by Moog's own admission, only required a search for the allegedly non-public information Moog identified. The Court should adopt Skyryse's proposed protocol and reject Moog's.

1. The Court Should Adopt Defendants' Proposed Forensic Protocol

"Forensic examinations of computers . . . are generally considered a drastic discovery measure because of their intrusive nature." *Aminov v. Berkshire Hathaway Guard Ins.*, 2022 WL 818944, at *1 (E.D.N.Y. Mar. 3, 2022); *see also Motorola Sols., v. Hytera Comm'ns Corp.*, 365 F. Supp. 3d 916, 925 (2019) ("Forensic examination of a party's computers . . . is no routine matter"). Even where good cause may exist for the production and imaging of computers, courts should "guard against undue intrusiveness resulting from inspecting or testing [them]." *Popat v. Levy*, 2021 WL 5166173, at *2 (W.D.N.Y. Nov. 5, 2021) (quoting Advisory Committee Notes, Fed. R. Civ. P. 34 (2006)); *Calyon v. Mizuho Sec. USA Inc.*, 2007 WL 1468889, at *6 (S.D.N.Y. May 18, 2007).

In trade secrets cases, courts generally seek to heed this directive by adopting protocols in which (i) an independent, neutral forensic examiner images the devices at issue pursuant to a confidentiality agreement; (ii) the examiner searches the images for potentially relevant documents using search terms agreed by the parties and provides documents to the producing

party for review as to privilege and responsiveness; and (iii) the producing party produces any non-privileged, responsive documents to the requesting party. *See, e.g.*, *Wynmoor Cmty. Council, Inc. v. QBE Ins. Corp*., 280 F.R.D. 681, 687–88 (S.D. Fla. 2012) (parties to agree on search terms to be used by independent examiner with producing party to review results and produce non-privileged, responsive documents to plaintiff); *Sony BMG Music Ent. v. Arellanes*, 2006 WL 8201075, at *1 (E.D. Tex. Oct. 27, 2006) (same); *Ameriwood Indus., Inc. v. Liberman*, 2006 WL 3825291, at *5 (E.D. Mo. Dec. 27, 2006) (ordering appointment of independent expert to image and recover all files from defendants' hard drives and provide them to defendants' counsel, with defendants to produce any non-privileged, responsive documents to plaintiff)*; see also, e.g.*, *Brocade Comm'ns Sys., Inc. v. A10 Networks, Inc.*, 2012 WL 70428, at *3 (N.D. Cal. Jan. 9, 2012) (providing if parties could not agree to inspection carried out by plaintiff's expert, supervised by defendant's expert, the parties shall "select[] a neutral third party expert to conduct the inspection," and in all events requiring "the forensic expert produce any recovered files to [defendant] first, to all [defendant's] counsel to review the files as to relevance, responsiveness, and privilege prior to any disclosure to [plaintiff]").

Skyryse's proposed protocol is consistent with this precedent. It provides that iDS will forensically image all physical devices delivered to iDS and search all recovered data for file attribute information Moog itself represented "is sufficient for Defendants to comply with the March 11, 2022 stipulated order." Ex. 5. This includes information relating to Moog's list of 136,994 records allegedly downloaded by Defendant Kim from Moog's systems (the "Moog Filename List") and Moog's list of 62,408 MD5 hash values associated with a subset of the Moog Filename List (the "Moog Hash Value List")—in each case, modified only to remove files that did not originate with or belong to Moog. *See* Ex. 1 (Sections II and III). Under Skyryse's protocol, iDS generates reports identifying the extent to which the foregoing files were stored on, used by, or transferred to or from the inspected devices, and all underlying data relied upon to generate the reports. *Id.* Those reports are provided to Skyryse's counsel for a privilege review, and produced two weeks later with any appropriate privilege redactions and a privilege log. *Id.* After proposing this protocol to Moog, Skyryse also offered during meet and confer to add a provision authorizing iDS to conduct searches using search terms agreed by the parties—in addition to searches using the Moog Filename and Hash Value Lists—to identify files for the reports. This procedure strikes the standard, appropriate balance between Moog's asserted need for discovery and Skyryse's right to protect its sensitive information and devices. *See, e.g.*, Order, *Peters v. Infor(US), Inc*., No. 3:19-cv-08102, Dkt. 64 (N.D. Cal. Apr. 20, 2021 (third-party neutral to search electronic devices using search terms and filename/hash lists)); Order, *Optiv Security Inc. v. Weiske*, No. 8:20-cv-01523, Dkt. 194 (C.D. Cal. Nov. 30, 2020 (third party forensic expert to determine if devices contained plaintiff's confidential intellectual property and/or proprietary information using search terms and defined list of plaintiff's data)).

2. The Court Should Reject Moog's Unprecedented Proposed Forensic Protocol

Despite the parties' agreement on a neutral forensic examiner for this case, Moog seeks to have *its own* expert and outside counsel *directly inspect* the devices instead. Ex. 2. This is an extraordinary request for unfettered access to Skyryse's information having nothing to do with the allegations in this case, and is directly contrary to the March 11 Order, which expressly states that the purpose of the neutral forensics firm is for delivery of information "*in lieu of* providing such information *directly to Plaintiff*." March 11 Order at 2. Moog's request for an

unbounded fishing expedition runs afoul of the principles embodied in the Federal Rules and case law that forensic inspection must minimize the burden on, and most effectively protect the confidential materials belonging to, the producing party. *Aminov*, 2022 WL 818944, at *1; *Popat*, 2021 WL 5166173, at *2; *Calyon*, 2007 WL 1468889, at *6.[1]

A. Moog's Request For Unfettered Access Is Not Proportionate To The Allegations And Information It Has Provided In this Case To Date

Moog has not yet identified the purported trade secrets it contends Defendants misappropriated. To date, Moog has provided Defendants only the Moog Filename and Hash Value lists—which, although demonstrably overbroad,[2] Moog represented were "sufficient for Defendants to comply with the March 11, 2022 stipulated order." Ex. 5. Nonetheless, Moog now claims its expert and outside counsel must directly inspect the devices in iDS's possession for information *beyond* that contained in the Moog Filename and Hash Value lists—extending to *all* non-privileged material on *all* the devices in iDS's possession. This is unprecedented and improper.

By Moog's own representation, the scope of Moog's proposed inspection far exceeds that which is necessary to comply with the March 11 Order. *See* Exs. 2, 4. Moog's proposed scope also is premature because Moog has not yet provided Defendants with any particularized identification of its purportedly misappropriated trade secrets—a prerequisite to the discovery it seeks. *See, e.g.*, *A&P Tech., Inc. v. Lariviere*, 2017 WL 6606961, at *9 (S.D. Ohio Dec. 27, 2017) (requiring particularized trade secret identification for DTSA claim before discovery where, as here, "[i]t is too early to tell whether . . . Moog's lawsuit is an attempt to use litigation as a means of discovery the trade secrets of a competitor"); *MSCI Inc. v. Jacob*, 945 N.Y.S.2d 863, 866 (N.Y. Sup. Ct. 2012) (barring plaintiffs from seeking further discovery until required identification made, including identifying for source code "which of the component parts or sequencing of their source code are not (1) publicly available information, (2) commonly-used algorithms, or (3) third-party licensing"). In these circumstances, it appears Moog's request for complete access to Skyryse devices—likely to include Skyryse source code and other highly sensitive and proprietary Skyryse information—is nothing more than an attempt to rummage through Skyryse's files to shore up Moog's deficient allegations and potentially claim *Skyryse's* confidential information and trade secrets as its own.

B. Moog's Purported Need For Skyryse's Source Code, Process Assets, and Forensic Data Does Not Justify The Intrusive Inspection Moog Seeks

Moog says Skyryse's proposed protocol is not workable because Moog needs access to (i) Skyryse's source code; (ii) "process assets," *i.e.*, documents Moog purports to have developed to provide a framework for ensuring its software complies with federal regulations;

---

[1] Moog's initial proposed protocol sought direct access to the forensic images of Skyryse's devices *before* giving Skyryse any opportunity to review the images for privilege. After Skyryse explained why such an approach was improper, Moog agreed to revise its protocol to permit Skyryse to review forensic images before they are produced to Moog and excise any privileged materials. Ex. 6.

[2] As Skyryse previously explained to Moog, both the Moog Filename and Hash Value Lists contain broad swaths of *public* information—including generic filenames readily found in *non-Moog* file systems because they are used or produced by common applications or are commercially available. Ex. 7.

and (iii) forensic data concerning the devices in iDS's possession. Ex. 3. Even if Moog was able to show it is entitled to this information (which it cannot do because it has not yet identified its purported trade secrets with reasonable particularity), all the information can be obtained through means less burdensome and prejudicial to Defendants than the unbounded access Moog seeks. In fact, Skyryse proposed means of providing Moog access to each of these three categories of information that would not require simply turning over full device images to Moog's expert and outside counsel. Ex. 4. Moog rejected each proposal without explanation.

Source Code. Skyryse explained that, if warranted, it could make its source code available on a source code computer pursuant to a source code protective order to be agreed by the parties, which is standard practice in technical trade secrets and patent cases.[3] *Id.* Moog does not need access to the full devices in iDS's possession to obtain Skyryse source code.

"Process Assets." Moog postulates that because the individual defendants may have misappropriated "process assets"—which it describes as including "templates, checklists, tools, [and] test cases" for specific government standards (e.g., "DO_178")—its experts and outside counsel need full access to the devices in iDS's possession to locate any such misappropriated "process assets." Not so. These files—like most allegedly misappropriated files in a trade secret case—can be identified through an agreed search protocol. For this reason, Skyryse offered to expand its proposed protocol beyond the Moog Filename and Hash Value Lists to additional search terms designed to located purported "process assets" Moog claims the individual defendants may have misappropriated. *Id.* Moog rejected that offer, insisting its expert must have full access to forensic images to compare process assets and determine if any similarities are the result of copying. This makes no sense. Under Moog's flawed reasoning, any time a defendant is accused of trade secret misappropriation it must provide unfettered access to devices because search terms are an imperfect means of capturing the plaintiff's proprietary information the defendant could have altered. That would grant every trade secret plaintiff *carte blanche* to obtain a competitor's most sensitive commercial information simply by filing a complaint, which is contrary to standard practice. *See, e.g.*, *Wynmoor Cmty.* 280 F.R.D. at 687–88; *Ameriwood Indus., Inc.*, 2006 WL 3825291, at *5; *Brocade Comm'ns Sys., Inc. v. A10 Networks, Inc.*, 2012 WL 70428, at *3. Moog knows the universe of process assets the individual defendants possibly could have taken and can propose search terms to identify those documents to the extent they exist on the devices in iDS's possession. That is the proper and sensible way to proceed.

Forensic Data. Moog says its expert must directly inspect the devices Skyryse provided to iDS in order to obtain standard forensic data, such as whether and when folders containing Moog information were accessed, viewed, edited, or transferred, and when any such information could have migrated to Skyryse's networks. *See* Ex. 2. Moog cannot explain why iDS—a top-tier forensics firm—is incapable of providing such standard information to Moog. If iDS identifies files based on search terms directed at Moog's purported confidential information and trade secrets, it can provide the basic forensic data for those files Moog seeks.

---

[3] *See generally Cincom Sys. v. Labware, Inc.*, 2022 WL 672644, at *1 (S.D. Ohio Mar. 7, 2022) and *Philips Med. Sys. Nederalnd B.V. v. TEC Holdings, Inc.*, 2021 WL 1234596, at *11 (W.D.N.C. Mar. 31, 2021) (discussing source code inspection protocols).

Moog has not provided any compelling justification for its unprecedented and overbroad forensic protocol. Neutral forensic examiners are standard in trade secrets litigation, and Moog has shown no reason its own expert and outside counsel must be permitted to take over that role in this case. Nor has Moog shown that search terms, file names, and hash values—standard forensic search mechanisms in a trade secrets case—are insufficient and must be supplanted with wholesale access to a competitor's devices and highly sensitive information. Moog plainly seeks to engage in a fishing expedition this Court should not endorse. Moog's proposed protocol should be rejected, and Skyryse's standard, sensible protocol order adopted.

AEO Provision of Proposed Protective Order

The parties have been actively negotiating a protective order. While they have agreed on nearly all aspects of the document, they have reached an impasse on the provision regarding treatment of Attorneys-Eyes-Only ("AEO") documents that requires the Court's intervention: Skyryse wants its employees to view Moog's AEO documents if they are a sender or recipient of the material, as is customary in trade secrets cases. Moog wants to limit the Skyryse employees that can view Moog's AEO documents to deponents.

Specifically, following the parties' April 15, 2022 meet and confer, Skyryse proposed an AEO provision that would allow the officers, directors, or employees of the corporate parties (i.e., Moog and Skyryse) to view AEO-designated documents, provided that (among other things) they are a sender, recipient, or author of those documents, or are specifically identified in the documents as having received a copy. Ex. 8. On April 18, 2022, Moog rejected this proposal, counter-offering an AEO provision that would allow the corporate parties' officers, directors, or employees to view AEO documents if they are a sender, recipient or author of the material—*and only if they have been noticed for deposition or identified as a 30(b)(6) deponent*. Ex. 9.

The Court should adopt Skyryse's proposed Protective Order and reject Moog's. Skyryse's AEO provision is consistent with those numerous courts have adopted in trade secrets cases. Moog's AEO provision, by contrast, prevents Skyryse from having a full and fair opportunity to mount its defense to Moog's dire allegations.

1. Skyryse's Proposal Represents the Standard Approach to AEO Disclosure in Trade Secrets Cases.

Numerous courts in the Second and Ninth Circuits have approved protective orders in trade secrets cases that broadly allow the disclosure of AEO materials to authors and recipients of documents, *including outside the context of depositions*. In *Better HoldCo, Incorporated v. Beeline Loans, Incorporated*, for example, the Southern District of New York approved a protective order that allowed disclosure of AEO material "as to any document, its author, its addressee, its custodian, and any other person shown on the face of the document or in the metadata as having received a copy." *Better HoldCo, Inc. v. Beeline Loans, Inc.*, No. 1:20-cv-08686, Dkt. 45 ¶ 10(d) (S.D.N.Y. Jan. 25, 2021). Other courts have routinely granted orders with substantially the same provisions. *See, e.g. SFM Realty Corp. v. Lemanski*, No.1:20-cv-00209, Dkt. 30 (S.D.N.Y. Jan. 21, 2020) (allowing disclosure of AEO material in trade secrets case to "any witness who counsel for a party in good faith believes may be called to testify at a hearing, trial or deposition in this action about the document and who is also an author,

recipient or copy recipient on the document"); *see also Upstrem, Inc. v. BHFO, Inc*., No. 3:20-cv-02160 (S.D. Cal. June 30, 2021), Dkt. 42, ¶ 6.3(f) (allowing disclosure of AEO material in trade secrets case to "any person indicated on the face of the document to be its originator, author or recipient of a copy of the document"); *Nalco Company LLC v. Bryan Carota,* No. 2:21-cv-04142 (C.D. Cal. Feb. 13, 2022) (allowing disclosure of AEO material in trade secrets case to "author or recipient of a document containing the information or a custodian or other person who otherwise possessed or knew the information"); *Wisk Aero LLC v. Archer Aviation Inc*., No. 3:21-cv-02450 (N.D. Cal. Oct. 06, 2021), Dkt. 161 ¶ 7.3(f) (same); *Philips North Am. LLC v. Advanced Imaging Servs., Inc*., No. 2:21-cv-00876, Dkt. 49¶ 7.3(g)(E.D. Cal. July 29, 2021) (same).

Skyryse's proposed AEO provision is even *narrower* than the protective orders adopted in these cases. In addition to limiting AEO material to the corporate parties' individual officers, employees, or directors who authored or received the material (or are indicated in the accompanying metadata as having received a copy), Skyryse has further agreed to limit the manner in which these materials may be disclosed to those individuals in the following ways:

- The disclosure of AEO material to the corporate parties' officers, directors, or employees must be made solely for a purpose related to this litigation;
- The disclosure must be made by counsel under circumstances where counsel can continuously observe the corporate parties' officer, director, or employee;
- Counsel must admonish the officer, director, or employee to refrain from taking screenshots or pictures of the material;
- The corporate party shall not be permitted to make or retain copies of any of the AEO material; and
- The disclosure shall be immediately surrendered to the custody of that Party's counsel, and shall automatically be treated as though any such materials were themselves material designated.

Ex. 8 at ¶ 6.5(k).

Skyryse's reasonable compromises in including the above restrictions ensure that Moog's interests in protecting the confidentiality of its AEO material are fully protected. The Court should adopt Skyryse's Protective Order.

2. Moog's Proposal Prevents Skyryse From Adequately Defending Itself In This Litigation

Despite Skyryse's compromises, Moog insists that the corporate parties' officers, directors, or employees may view AEO material *only* if they have been noticed for deposition or designated as a Rule 30(b)(6) representative. Ex. 9. This is unworkable. Skyryse is currently facing grave (albeit meritless) trade secret misappropriation allegations and numerous other claims. Skyryse should be able to consult with those who are already familiar with Moog's AEO material to test the veracity of Moog's claims—and Skyryse should be able to do so at any time, not merely once depositions have been noticed. Skyryse's ability to share AEO material

with its employees for the purpose of investigating Moog's claims and building Skyryse's defenses should not depend upon on whom Moog chooses to depose.

Moreover, Moog's purported interest in protecting its AEO material from former Moog employees at Skyryse is fully addressed by Skryse's commitment that only individuals who authored or received the AEO material may view it, in the strict supervision of counsel, and pursuant to the additional limitations noted above. The knowledge of an individual who authored or received a document may be important to Skyryse's ability to understand the material and its context, and therefore to prepare Skyryse's defense. That is the case regardless of whether—or when—the individual has been noticed for deposition.

Moog also previously indicated during the parties' April 15 meet and confer that limiting Skyryse's ability to show AEO materials to only deponents is necessary as a matter of fairness. Moog says that because numerous former Moog employees left to work at Skyryse, while no former Skyryse employees work at Moog, Skyryse gets an unfair, non-reciprocal advantage in having its employees view Moog's AEO material. That Moog does not have former Skyryse employees to view Skyryse's AEO material, however, is not the result of some "unfair advantage"—but rather the reality that *Moog* is accusing *Skyryse* of poaching its employees and misappropriating Moog's confidential information and trade secrets, and not the other way around. Moog does not need its employees to view *Skyryse's* AEO-designated material to support its claims—Moog only needs to be able to identify *Moog's* information to the extent it infiltrated Skyryse's systems. In contrast, it may be material to Skyryse's defense to understand the context of a document Moog has marked AEO, and if a Skyryse employee has already been privy to the information through employment at Moog, there is no reason Skyryse should not be able to show the individual the information to assist in mounting a defense. Moog has yet to cite any authority supporting its contrived fairness argument, and Skyryse is aware of none.

The only apparent rationale for Moog's attempt to limit Skyryse's ability to show AEO material to individuals who have already sent or received it to the context of deposition preparation is to hinder Skyryse's ability to attack Moog's claims throughout the entirety of this litigation. Because Moog's AEO provision is thus prejudicial to Skyryse—and lacks any legitimate basis given the additional protections afforded by both parties' proposed Protective Orders—the Court should reject it, and adopt Skyryse's proposed Protective Order.

Sincerely,

Kate Dominguez